

Security Guidelines for the Electricity Sector: Physical Security

Effective Date: TBD Pending BOT Approval	Version: 2.0
	Approved by Board of Trustees: May 2007

Preamble

This guideline reviews the concepts an electricity sector organization should consider when implementing physical security measures to safeguard personnel and prevent unauthorized access to critical equipment, systems, material, and information at or pertaining to critical facilities.

Introduction

The Physical Security guideline provides electricity sector organizations with basic physical security concepts and the measures to consider when implementing a physical security program. The foundation of any company's physical security program is the physical security measures implemented to protect company personnel, assets, and information. Each organization should decide on the scope of the physical security measures implemented at its various facilities.

Purposes

As the foundation of any company's security program, physical security measures help ensure the safety and security of a company's personnel, assets, and information. By providing the basic concepts of physical security and common measures available to electric sector organizations, the guideline should enable companies to develop a physical security plan that matches the level of accepted risk for each of their critical facilities.

Applicability

This guideline applies to facilities and functions that are considered critical to the support of the electricity infrastructure and the overall operation of the individual organization. Each electricity sector organization is expected to define and identify those facilities and functions it believes to be critical, keeping in mind that the ability to mitigate the loss of a facility or function through redundancies may make some facilities less critical than others. From an industry wide perspective, a critical facility or function may be defined as any facility, function, or combination thereof that, if severely damaged or destroyed, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact to the reliability or operability of the energy grid, or would cause significant risk to public health and safety.

Guideline Statement

This guideline describes the basic physical security concepts, measures, and the common practices" that may be implemented by electricity sector organizations for facilities or functions identified as critical.

Guideline Detail

Physical Security Concepts Overview

Physical security typically comprises eight distinct concepts, these are:

- **Deter** – visible physical security measures installed to induce individuals to seek other less secure targets.
- **Detect** – physical security measures installed to detect unauthorized intrusion and provide local and/or remote intruder annunciation.
- **Delay** – physical security measures installed to delay an intruder’s access to a physical asset and provide time for incident assessment and response.
- **Assess** – the process of evaluating the legitimacy of an alarm and the procedural steps required to respond.
- **Communicate** – communication systems utilized to send and receive alarm/video signals and voice and data information. Also, includes the documented process to communicate detected intrusions.
- **Respond** – the immediate measures taken to assess, interrupt, and/or apprehend an intruder.
- **Intelligence** – measures designed to collect, process, analyze, evaluate and interpret information on potential threats.
- **Audit** – the review and inspection of physical security measures to evaluate effectiveness.

Together, these concepts, if applied, provide a consistent “systems approach” to designing and implementing physical security measures that will mitigate the impact on critical assets should a physical attack occur.

Prior to implementing a physical security program, each organization should prioritize its facilities and assets by characterizing risks based on factors such as:

- Prior history of incidents;
- Threat warnings from law enforcement agencies;
- System redundancies; and
- Overall operating requirements

After the facilities and assets have been prioritized, the asset owner can then plan for and implement the physical security measures they consider appropriate to the identified risk.

In designing a physical security program, the objective of the aggressor should be considered. Four objectives in describing an aggressor’s intent that should be considered are:

Physical Security Guideline Version 2.0: Effective July 1, 2007

- Destroying or damaging critical facilities, property, or equipment;
- Stealing or damaging critical equipment, materials, or information;
- Posing a threat to the safety of personnel or customers; and
- Creating adverse publicity and inducing panic

To ensure the effectiveness of installed or procedural security measures, each organization should also consider an inspection and survey program to review existing security systems and procedures and make recommendations for appropriate changes as necessary.

Common Physical Security Systems and Processes

Determining the types of physical security measures and processes required can be complicated by the many options available. When designing, implementing, or auditing a physical security program, organizations should consider the following:

- Fencing, gates, or other barriers to restrict access to the facility;
- Limiting access to authorized persons through measures such as unique or restricted keying systems, “smart locks,” access card systems, or the use of security personnel;
- Access control measures to identify and process all personnel, visitors, vendors, and contractors, (i.e. photo IDs, visitors passes, contractor IDs displayed by all personnel while on company property);
- Internal alarm systems to monitor entry into control rooms or other critical buildings or areas;
- Perimeter or area alarm systems to monitor unauthorized intrusion into a facility’s outer perimeter barrier;
- Recorded closed circuit television systems (CCTV) that can provide local and/or remote surveillance capability of a protected facility;
- Roving security patrols or fixed station security staffing;
- Integrated alarm, CCTV, and other security systems, that report locally or to a central alarm station, that can be assessed and the appropriate company or law enforcement personnel dispatched to investigate a potential problem;
- Vehicle barriers to delay or stop vehicles;
- Projectile barriers to project vulnerable equipment or personnel;
- Security survey and other risk assessment program;
- Lighting that provides visibility for observation and optimum CCTV functionality;
- Signage to warn potential intruders; and
- Comprehensive security awareness program.
- The levels of physical security measures may be increased or lowered based on changes in threat levels, evolving threat scenarios, and facility risk categories.

Physical Security Guideline Version 2.0: Effective July 1, 2007

- This function may be served by the utilities threat alert plan developed to coordinate with the U.S. Department of Homeland Security's Advisory System or the advisories issued by the Public Safety and Emergency Preparedness Canada (PSEPC) of Canada.

Related Documents

Security Guidelines for the Electricity Sector:

<http://www.esisac.com/library.htm>:

- Guideline Overview
- Vulnerability and Threat Assessment
- Emergency Plans
- Continuity of Business Practices
- Communications
- Employment Background Screening
- Protecting Potentially Sensitive Information
- Threat and Incident Reporting
- Physical Security - Substations
- Physical Response

An Approach to Action for the Electricity Sector, Version 1, NERC, June 2001,

<http://www.nerc.com>

Threat Alert Levels and Physical Response Guidelines, NERC, November, 2001,

<http://www.nerc.com>

Threat Alert Levels and Cyber Response Guidelines, NERC, March 2002,

<http://www.nerc.com>

NERC Sabotage Reporting Standard CIP 001,

http://www.nerc.com/~filez/standards/Reliability_Standards.html#Critical_Infrastructure_Protection

NERC Cyber Security Standards CIP 002 – CIP 009,

http://www.nerc.com/~filez/standards/Reliability_Standards.html#Critical_Infrastructure_Protection

Risk Assessment Methodologies for the Electric Sector, NERC, September 2005,

<http://www.esisac.com/library.htm>

**Physical Security Guideline
Version 2.0: Effective July 1, 2007**

Revision History

Effective Date	Version Number	Reason/Comments
6/14/2002	1.0	Initial Version
7/1/2007	2.0	Extensive updates and edits to make the text current and to incorporate the 2006 CIPC approved format for all guidelines.
<p>NOTE: This Physical Security Guideline will remain in effect until it is either changed or rescinded by NERC. The guideline will be reviewed:</p> <ul style="list-style-type: none">• ...following any significant change in the Electricity Sector that warrants review and updating of this guideline, or• ...three years following the guideline's Effective Date.		